



Magyar mobilosok, vigyázat: csalók utaznak a pénzükre!

Mostanában újra divatba jöttek a hamis számlabekérők: ne dőljön be nekik, és inkább kétszer nézze át, valódi számlát kapott-e a tényleges szolgáltatótól.



Már a Telenor és a Telekom is közleményben figyelmeztetik ügyfeleiket arra, hogy e-mailben hamis számlabekérőket kaphatnak, amely egy szolgáltatótól független weboldalra irányítja őket, hogy aztán a pénzükbánja a figyelmetlenséget. Persze közben a mobilszámuk se lesz befizetve.

A szolgáltatók figyelmeztetései szerint hozzájuk is érkezett az ügyfelektől visszajelzés csalásokról, és a közösségi médiában is egyre több információ található hasonló, átverős e-maillal megtévesztett mobiltelefon-használókról. Nem ez az első csalárd módon pénzhez jutási próbálkozás, de a megtévesztő e-mailekkel trükközők – a látványra, megjelenésre is figyelemmel – igyekeznek valóban hasonló, ezáltal hitelesnek tűnő hátteret kanyarítani.

Az e-mail első pillantásra valóban a szolgáltató által kibocsátottnak tűnik. Számla kiegyenlítésére, vagy az adatok frissítésére kéri az ügyfelet.

Erre a levélben egy webes hivatkozás található, mely jelentősen hasonlít távközlési cég elérhetőségére, de valójában egy ügyes „eltérítés” van a link, hivatkozás mögött.

TISZTELT ÜGYFELÜNK

A számlát nem fizették még :

Folyószámla : 363800069.
Számla sorszám : 5120170015337201
Fizetési határidő : 24/04/2018

Státusz : Befizetésre vár

Számlázott összeg : 1.315 Ft

Remeljük, hogy a számla kifizetése a megadott határidőn belül. Vagy az eA fizetés velünk automatikusan kikapcsol

Most már fizetni a számlákat egyszerű és sima utat a bankkártya vagy a bankszámla es biztonságosan

Kerjük, kövesse az alábbi linket a folyamat befejezéséhez

<https://www.telekom.hu/telekomfiok/belepes?6...../Token=252MSBTKL55....ID>

©2018 Magyar Telekom Nyrt.

(A szöveget figyelmesen olvasva szembetűnő a magyartalan fogalmazás!)



Mi történhet, ha sikerül az átverés?



* A szolgáltató számlájához megtévesztően hasonló számlát küldenek, az azon szereplő számlaszám viszont a csalóké. Ha az összeg nem kirívóan magas, többen odafigyelés nélkül, rutinszerűen fizetnek, amiből a csalók gazdagodnak. A szolgáltatóhoz ebből természetesen egy fillér se kerül.

* Az adategyeztető oldalon elkérik a belépési adatokat (például név, jelszó, telefonszám), amelyek a szolgáltató alkalmazásaiba (pl. a MyTelenor appba) is belépést biztosítanak. Ezen keresztül pedig a megtévesztett személy nevében

rendelhetnek akciós, hűségpontos, vagy épp részletfizetéses készülékeket – természetesen saját részre – a részletfizetést viszont az adat regisztrált birtokosának kell teljesítenie.

* Számlaegyeztetés céljából elkérik a mobilszámlája másolatát, ezzel pedig megint csak úgy tudnak visszaélni, hogy az Ön nevében kommunikálnak a szolgáltató felé, és rendelhetnek termékeket vagy szolgáltatásokat.

☞ A szolgáltatók a fenti trükkök terjedésének megakadályozása miatt arra kérik az ügyfeleket, hogy sokkal óvatosabbak legyenek azokkal a levelekkel és akár telefonhívásokkal, amelyek látszólag tőlük érkeznek.

☞ Minden esetben hasonlítsa össze a feladót vagy a hívószámot, és csak akkor higgyen a szolgáltató kilétének azonosságában, ha az eddigi e-mail címről vagy számról keresik Önt.

☞ Ha bármilyen gyanú merülne fel, inkább hívja a távközlési cégek információs telefonszámait, vagy nézze meg a kapcsolódó adatokat a szolgáltató hivatalos alkalmazásában. Ha például kap egy valódinak tűnő számlát 5.900,- Ft-ról, de pl. a MyTelenor appban egyetlen 8.000,- Ft-os számlát lát, egyértelmű lehet, hogy a beérkező kérést csaló küldte.



A szolgáltatók igyekeznek letiltani a csaló weboldalak elérését saját hálózatukon belül, de az a legegyszerűbb és legjobb megoldás, ha Ön – még befizetés előtt – alaposan, nagyobb figyelemmel ellenőrzi a beérkező számlát.

Forrás: www.pcworld.hu
Képek: internet